IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

Applicants : Harry Snyder et al.

Serial No. : 10/758,984

Filed : January 16, 2004

For : EXECUTABLE APPLICATION ACCESS MANAGEMENT SYSTEM

Examiner : Hung T. Vy

Art Unit : 2163

APPEAL BRIEF

May It Please The Honorable Board:

Appellants initiate a new appeal under 37 CFR 41.27 in response to the Final Rejection, dated December 27, 2007, of claims 1-19 of the above-identified application. The fee of five hundred ten dollars ($510.00) for filing this Brief is to be charged to Deposit Account No. 19-2179. Enclosed is a single copy of this Brief.

Please charge any additional fee or credit any overpayment to the above-identified Deposit Account.

Appellants do not request an oral hearing.

I. REAL PARTY IN INTEREST

The real party in interest of Application Serial No. 10/758,984 is the Assignee of record:

Siemens Medical Solutions Health Services Corporation
51 Valley Stream Parkway
Malvern, PA 19355-1406
which merged into Siemens Medical Solutions USA Inc. on 1 January 2007.

II. RELATED APPEALS AND INTERFERENCES

There are currently, and have been, no related Appeals or Interferences regarding Application Serial No. 10/758,984.

III. STATUS OF THE CLAIMS

Claims 1-19 are rejected and the rejection of claims 1-19 are appealed.

IV. STATUS OF AMENDMENTS

All amendments were entered and are reflected in the claims included in Appendix I.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 provides a system enabling individual organizations of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider (page 2, lines 17-20; page 9, lines 27-30; Fig. 1, reference no. 100). At an application service provider site (page 5, lines 10-13; page 11, lines 24-26; Fig. 1, reference no. 121), at least one database (page 5, lines 6-7; Fig. 1, reference no. 124) is included. The at least one database contains data representing a plurality of user interface images associated with a corresponding plurality of organizations (page 2, lines 20-21). The at least one database also contains data representing a plurality of executable procedures (page 10, lines 2-4; Fig. 1, reference no. 142) associated with the corresponding plurality of user interface images (page 2, lines 21-22; Fig. 1, reference no. 140). An executable procedure supports a user of a particular organization (page 10, lines 3-5; Fig. 1, reference no. 104) of the plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by the plurality of organizations (page 2, lines 23-25). A command processor (page 10, lines 6-9; Fig. 1, reference no. 134) employs at least one database for initiating execution of a particular executable procedure in response to a command initiated at a remote location associated with the particular organization using a particular user interface image associated with the particular executable procedure with the particular organization (page 2, lines 25-28). The particular executable procedure supports

the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to the particular organization without intervention by the application service provider (page 10, lines 9-14) and excluding access to the application data specific to the particular organization by employees of organizations other than the particular organization (page 2, lines 28-30; page 10, lines 17-21).

Dependent claim 3 includes all the features of independent claim 1, along with the additional feature the particular executable procedure and the particular user interface image are specifically associated with the particular organization. The authorization processor page 9, lines 1-3; page 9, lines 7-9; Fig. 1, reference no. 136) excludes access of the user and employees of the particular organization to user interface mages and executable procedures and data associated with organizations other than the particular organization (page 2, lines 28-30; page 10, lines 11-21).

Dependent claim 4 includes all the features of independent claim 1, along with the additional feature that the authorization processor excludes access to the user and employees of the particular organization to data associated with organizations other than the particular organization by removing permission of the user and employees of the particular organization to access the data associated with the other organizations from a directly of permissions used to control data access (page 10, lines 16-21).

Dependent claim 6 includes all the features of independent claim 1, along with the additional feature that the authorization processor removes the permission of the user and employees of the particular organization in response to addition of the particular organization as a new organization of the plurality of organizations (page 10, lines 23-25).

Dependent claim 8 includes all the features of independent claim 1, along with the additional feature that an executable procedure enables the user to at least one of: add an employee and remove an employee, of an organization as a user entitled to access the application hosted by the application service provider (page 11, lines 8-10).

Dependent claim 12 includes all the features of independent claim 1, along with the additional feature that the authorization processor uses a combination of an organization specific identifier and received employee identification information in providing an employee access to the application hosted by the application service provider to prevent replication of user identification information between two employees of different organizations of the plurality of organizations (page 10, line 29-page 11, line 2).

Independent claim 16 provides a system enabling an individual organization of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider (page 2, lines 17-20; page 9, lines 27-30; Fig. 1, reference no. 100). At an application service provider site (page 5, lines 10-13; page 11, lines 24-26; Fig. 1, reference no. 121), a communication processor (page 9, lines 1-7; Fig. 1, reference no. 132) for accessing at least one database (page 5, lines 6-7; Fig. 1, reference no. 124) is included. The at least one database contains data representing a plurality of user interface images that are associated with a corresponding plurality of organizations and a plurality of executable procedures (page 10, lines 2-4; Fig. 1, reference no. 142) that are associated with the corresponding plurality of user interfaces images (page 2, lines 21-22; Fig. 1, reference no. 140). An executable procedure supports a user of a particular organization (page 10, lines 3-5; Fig. 1, reference no. 104) of the plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by the plurality of organizations (page 2, lines 23-25). At least one repository includes data representing an application and associated application data specific to the particular organization (page 8, lines 3-9; page 29, lines 4-6). A command processor (page 10, lines 6-9; Fig. 1, reference no. 134) is included for using the communication processor in initiating execution of a particular organization specific executable procedure in response to a command initiated at a remote user suite associated with the particular organization using a particular organization specific user interface image communicated to the user site (page 2, lines 25-28). The particular user interface image is associated with the particular executable procedure and with the particular organization. The particular executable procedure supports the user in managing and granting access of an employee of the particular organization to the application and the associated application data specific to the particular organization (page 10, lines 9-14) following login (page 16, lines 8-10; Fig. 2, reference no. 200) to the application and without intervention by the application service provider and excludes access to the application data specific to the particular organization by employees of the organizations other than the particular organization (page 2, lines 28-30; page 10, lines 17-21).

Independent claim 17 provides a system enabling individual organizations of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider (page 2, lines 17-20; page 9, lines 27-30; Fig. 1, reference no. 100). At an application service provider site (page 5, lines 10-13; page 11, lines 24-26; Fig. 1, reference no. 121), at least one database (page 5, lines 6-7; Fig. 1, reference no. 124) contains data representing an image associated with a corresponding plurality of organizations and a plurality of executable procedures (page 10, lines 2-4; Fig. 1, reference no. 142) associated with the corresponding plurality of user

interface images (page 2, lines 21-22; Fig. 1, reference no. 140). An executable procedure supports a user of a particular organization (page 10, lines 3-5; Fig. 1, reference no. 104) of the plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by the plurality of organizations (page 2, lines 23-25). At least one repository includes data representing an application and associated application data specific to the particular organization (page 8, lines 3-9; page 29, lines 4-6). An authorization processor (page 9, lines 1-3; page 9, lines 7-9; Fig. 1, reference no. 136) authorizes access of the user to a particular user interface image and an associated particular executable procedure associated with the particular organization in response to received identification information of the user (page 10, lines 9-14) and excludes access of the user and employees of the particular organization to user interface images and executable procedures and data associated with the organizations other than the particular organization (page 2, lines 28-30; page 10, lines 17-21). A command processor (page 10, lines 6-9; Fig. 1, reference no. 134) employs the at least one database for initiating execution of a particular executable procedure in response to a command initiated at a remote location associated with the particular organization using a particular user interface image associated with the particular executable procedure and with the particular organization (page 2, lines 25-28). The particular executable procedure supports the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to the particular organization (page 10, lines 9-14) without intervention by the application service provider and excludes access to the application data specific to the particular organization by employees of organizations other than the particular organization (page 2, lines 28-30; page 10, lines 17-21).

Independent claim 19 provides a user interface system enabling individual organizations of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider (page 2, lines 17-20; page 9, lines 27-30; Fig. 1, reference no. 100). At an application service provider site (page 5, lines 10-13; page 11, lines 24-26; Fig. 1, reference no. 121) and accessed via a firewall (page 15, line 31-page 16, line 2; Fig. 1, reference no. 110), at least one database (page 5, lines 6-7; Fig. 1, reference no. 124) is included. The at least one database contains data representing a plurality of sets of user interface images associated with a corresponding plurality of organizations and a plurality of executable procedures (page 10, lines 2-4; Fig. 1, reference no. 142) associated with the corresponding plurality of sets of user interface images. An executable procedure supports a user of a particular organization (page 10, lines 3-5; Fig. 1, reference no. 104) of the plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by the plurality of

organizations (page 2, lines 23-25). A command processor (page 10, lines 6-9; Fig. 1, reference no. 134) employs the at least one database for initiating execution of a particular executable procedure in response to a command initiated at a remote location associated with the particular organization using a user interface image selected from a set of images associated with a particular organization (page 2, lines 25-28). The particular executable procedure supports the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to the particular organization (page 10, lines 9-14) without intervention by the application service provider and excludes access to the application data specific to the particular organization by employees of organizations other than the particular organization (page 2, lines 28-30; page 10, lines 17-21).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-3, 7 and 10-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Llewellyn et al. (U.S. Patent Pub. No. 2003/0061279 A1), hereinafter "Llewellyn."

Claims 4-6, 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Llewellyn (U.S. Patent Pub. No. 2003/0061279 A1) in view of Gavrila et al. (U.S. Patent Pub. No. 2002/0026592 A1), hereinafter "Gavrila."

VII. ARGUMENT

Applicants respectfully submit that Llewellyn does not anticipate the features claimed in claims 1-3, 7 and 10-19 of the present arrangement. Additionally, Applicants respectfully submit that Llewellyn, when taken alone or in combination with Gavrila, does not make the features claimed in claims 4-6, 8 and 9 unpatentable. Thus, reversal of the Final Rejection (hereinafter termed "rejection") of claims 1-19 under 35 U.S.C. 102(e) and 35 U.S.C. 103(a) is respectfully requested.

Rejection of claims 1-3, 7 and 10-19 under 35 U.S.C. 102(e)

Reversal of the rejection of claims 1-3, 7 and 10-19 under 35 U.S.C. 102(e) as being anticipated by Llewellyn (U.S. Patent Pub. No. 2003/0061279 A1) is respectfully requested because the rejection makes crucial errors in interpreting the cited reference. The rejection erroneously states that claims 1-3, 7 and 10-19 are anticipated by Llewellyn.

Overview of the Cited References

Llewellyn describes an apparatus that enables remote access and control of applications. The processing of the application takes place in multiple locations including a server whereon the application is installed and a workstation of a user. The workstation

typically provides user interface processing and the server handles the execution of the application. The apparatus may provide efficient use of resources by reducing the amount of data that must be passed between the workstation and the server. The apparatus may include applications enabling multiple users to access and control the same instance of a running application. The apparatus may also allow a provider to see a user's screen and control the computer of a user (*see* Abstract).

Gavrila describes a method for automatic permission management in centralized and distributed operating systems using role-based access control that supports selective and multiple instantiations of roles, multiple inheritance of permission and membership, and provides scalable and efficient distribution, review, and revocation of permissions and access authorization. Gavrila provides, in a further aspect, automatic propagation of updates of role-permission hierarchies to the access control lists of all objects affected by such updates. Gavrila provides, in yet a further aspect, per-role and per user review of permissions and requires neither redundant storage and additional administrative actions nor exhaustive searches of system resources. Gavrila makes use, in yet a further aspect, of both local and global groups for the instantiation of roles on multiple computer hosts, to implement nested groups and to enable the integration of extant host computers, which include local user accounts and groups defined on independent servers and workstations, within large distributed operating systems. In yet a further aspect, Gavrila provides the transition from an extant system state to an RBAC system state whereby permissions of users and groups to objects are managed centrally and automatically using roles, and removes the redundant user permissions to objects of a given state in the transition to the RBAC state (*see* Abstract).

CLAIMS 1, 2, 7, 10, 11 and 13-15

The present claimed arrangement provides a system enabling individual organizations of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider. At an application service provider site, at least one database is included. The at least one database contains data representing a plurality of user interface images associated with a corresponding plurality of organizations. The at least one database also contains data representing a plurality of executable procedures associated with the corresponding plurality of user interface images. An executable procedure supports a user of a particular organization of the plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by the plurality of organizations. A command processor employs at least one database for initiating execution of a particular executable procedure in response to a command initiated at a remote location associated with the particular organization using a particular user interface image

associated with the particular executable procedure with the particular organization. The particular executable procedure supports the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to the particular organization without intervention by the application service provider and excluding access to the application data specific to the particular organization by employees of organizations other than the particular organization. Llewellyn does not anticipate the features claimed in claim 1 of the present arrangement.

Llewellyn describes enabling remote access and control of applications located at multiple locations. Multiple users can access and control the same instance of a running application. A provider of a particular service may see a user's screen and control the computer of a user. Llewellyn does not disclose or suggest a "particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization following login to said application and without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 1 of the present arrangement. Llewellyn, contrary to the present arrangement, employs an administrator of a server farm (*see* fig. 2, reference no. 99) such as an **application service provider administrator** to manage user accounts. Llewellyn describes

> "an application program that would execute entirely on a server computer and enable one remote user to see and control the screen of a second remote user. Such a system would preferably include ... the ability for multiple users of an application to use a single instance of the application ... providing a distinct functionality or functionalities to the second and subsequent remote users" (paragraph [0027]).

Thus Llewellyn merely allows an application service provider to access an application program. Therefore, Llewellyn neither discloses nor suggests a "particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization following login to said application and **without intervention by the application service provider**" or "**excluding access** to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 1 of the present arrangement.

In the present claimed arrangement, "system 100 enables individual organizations 104 of multiple different organizations to manage access of employees to a remotely located

application 123 hosted by an application service provider" (specification, page 9, lines 27-29). Thereby:

> "The customer account management (CAM) system 100 **advantageously** provides efficient and secure intranet and Internet access for customer administrators at organizations 104, such as hospitals, to **manage their own application user accounts**. The system 100 restrict access so that customer account administrators have no access to user accounts assigned to other organizations, preferably by adding a prefix representing the parent organization in order to establish uniqueness. The system 100 permits customers to **self-sufficient to manage their own application user accounts, without requiring intervention** by or cooperation with another party. The system 100 provides real time savings for customers, and requires less staff time at the ASP support help desk to perform account management functions" (specification, page 31, lines 7-16).

Thus, the present claimed arrangement recites a "particular executable procedure" that supports a "user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization **without intervention by the application service provider** and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization." This is neither suggested nor disclosed by the system of Llewellyn.

> Moreover, Llewellyn in cited paragraph [0109] describes that
>
> "[t]he server configuration module 196 may enable an **administrator** of a server station 100 to specify security measures for a server. Security measures may include permissions for accessing files or functionality of a server module 160. The server configuration module 196 may also enable an administrator to **set up accounts** which may include authentication and configuration data associated with a particular user or **organization**" (paragraph [0109]).

Thus, the "administrator of a server station 100" is an Application Service Provider administrator and the administrator controls the operations performed by the system of Llewellyn. Therefore, Llewellyn **teaches directly away** from the claimed "user of a particular organization of said plurality of organizations in managing access ... **without intervention by the application service provider**." Moreover, Llewellyn in paragraph [0077] describes "[a] server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide **centralized administration** and horizontal scaleability." This is wholly unlike and is in direct contrast to the distributed access management by users of individual particular organizations "of said plurality of organizations in managing access of employees of the particular organization to an application hosted by an

application service provider and used by said plurality of organizations" as recited in claim 1 of the present arrangement.

Furthermore, Llewellyn teaches the advantages of centralized management of user access and fails to recognize the problem addressed by the claimed arrangement. Specifically, Llewellyn states:

> [t]he server farm 99 may be an Application Service Provider ('ASP') farm 99. **An ASP typically deploys, hosts, and manages access to an application**, such as an application 86, to multiple users from a centrally managed facility. An ASP also typically delivers applications 86 over networks 30, 50 on a subscription basis. Moreover, **ASPs are designed to speed implementation of new applications, minimize the expenses and risks borne over an application's life cycle**, and ameliorate the problems associated with the current shortage of qualified technical personnel in the marketplace" (paragraph [0078]).

Thus, in Llewellyn, an ASP manages access to an application. Moreover, Llewellyn describes the "[b]enefits of **application server computing** include **single-point management**, universal application access, bandwidth-independent performance, and **improved security** for business applications" (paragraph [0077]). Therefore, Llewellyn is concerned with "a system administrator [that] may be a provider [i.e. Application Service Provider] ... while the users of the system may be subscribers," (paragraph [0193]). Llewellyn neither discloses nor suggests "the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization **without intervention by the application service provider** and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 1 of the present arrangement.

Furthermore, cited paragraph [0092] of Llewellyn describes that "[t]he entry point management module 148 may also maintain connections between users and entry points, allowing users to access data and functionality specific to their session with an application 86." Cited paragraph [0176] describes that "[e]ach user interface 482a,b may be different and allow access to data 484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a." However, as described above, the system of Llewellyn is managed by an Application Service Provider. Therefore, Llewellyn neither discloses nor suggests "the particular executable procedure supporting the user in managing

and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 1 of the present arrangement. Consequently, it is respectfully requested that the rejection of claim 1 under 35 U.S.C. 102(e) be withdrawn.

In view of the above remarks, Applicants respectfully submit that Llewellyn does not anticipate the features claimed in the present claimed arrangement. Additionally, as claims 2, 7, 10, 11 and 13-15 are dependent on independent claim 1, these claims are considered patentable for the reasons presented above with respect to claim 1. Consequently, it is respectfully submitted that the rejection of claims 2, 7, 10, 11 and 13-15 under 35 U.S.C. 102(b) be withdrawn.

CLAIM 3

Dependent claim 3 is dependent on independent claim 1 and is considered patentable for the reasons presented above with respect to claim 1. Additionally, claim 3 is also considered patentable because the features claimed are not anticipated by Llewellyn. Specifically, Llewellyn neither discloses nor suggests that "the authorization processor excludes access of the user and employees of the particular organization to user interface images and executable procedures and data associated with organizations other than the particular organization" as recited in claim 3 of the present arrangement. The Office Action cites paragraphs [0109] and [0077] of Llewellyn as being relevant to the present arrangement. Applicants respectfully disagree. The cited passages merely describe that a "[s]erver configuration module 196 may enable an administrator of a server station 100 to specify security measures for a server. Security measures may include permissions for accessing files or functionality of a server module 160. The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization" paragraph [0109]. Cited passage [0077] describes

> "A server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide centralized administration and horizontal scaleability. The server farm 99 may provide application server computing support to an enterprise or other selected entity or entities. Application server computing may be defined as a server-based approach to delivering applications to end-user devices. **Benefits** of application server computing include **single-point** management, universal application access, bandwidth-independent performance, and improved security for business applications."

However, this fails to show or suggest the claimed authorization processor which "excludes access" to "user interface images and executable procedures and data associated with organizations other than the particular organization" as in the present claimed arrangement. Llewellyn may describe enabling an administrator to set up accounts which include authentication and configuration data associated with a particular user or organization, however, the authentication does not specifically exclude access to "**user interface images** and **executable procedures** and data associated with **organizations other than the particular organization**" as recited in claim 3 of the present arrangement. Therefore, Applicants respectfully submit that Llewellyn does not anticipate the present invention claimed in claim 3. Consequently, it is respectfully submitted that the rejection of claim 3 under 35 U.S.C. 102(b) be withdrawn.

CLAIM 12

Dependent claim 12 is dependent on independent claim 1 and is considered patentable for the reasons presented above with respect to claim 1. Additionally, claim 12 is also considered patentable because the features claimed are not anticipated by Llewellyn. Specifically, Llewellyn neither discloses nor suggests that "the authorization processor uses a combination of an organization specific identifier and received employee identification information in providing an employee access to the application hosted by the application service provider to prevent replication of user identification information between two employees of different organizations of the plurality of organizations" as recited in claim 12 of the present arrangement. The Office Action asserts that Llewellyn describes "identifying a user or identifying others associated with a user ... authorization data 272 may include data indicating things that a user is authorized to do or places that a user is authorized to access" in paragraph [0124] and that "[t]he server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization" in paragraph [0109]. Although Llewellyn may describe identifying a user and authenticating a user, Llewellyn neither discloses nor suggests "prevent[ing] replication of user identification information between two employees of different organizations of the plurality of organizations" as recited in claim 12 of the present arrangement. Llewellyn merely describes authorizing access to a user or others associated with a user. However, Llewellyn does not recognize the problem of "replication of user identification information between two employees of different organizations." Therefore, Llewellyn neither discloses nor suggests "prevent[ing] replication of user identification information between two employees of different organizations of the plurality of organizations" as recited in claim 12 of the present arrangement. Consequently, it is respectfully submitted that the rejection of claim 12 under 35 U.S.C. 102(b) be withdrawn.

CLAIM 16

Independent claim 16 provides a system enabling an individual organization of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider. At an application service provider site, a communication processor for accessing at least one database is included. The at least one database contains data representing a plurality of user interface images that are associated with a corresponding plurality of organizations and a plurality of executable procedures that are associated with the corresponding plurality of user interfaces images. An executable procedure supports a user of a particular organization of the plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by the plurality of organizations. At least one repository includes data representing an application and associated application data specific to the particular organization. A command processor is included for using the communication processor in initiating execution of a particular organization specific executable procedure in response to a command initiated at a remote user suite associated with the particular organization using a particular organization specific user interface image communicated to the user site. The particular user interface image is associated with the particular executable procedure and with the particular organization. The particular executable procedure supports the user in managing and granting access of an employee of the particular organization to the application and the associated application data specific to the particular organization following login to the application and without intervention by the application service provider and excludes access to the application data specific to the particular organization by employees of the organizations other than the particular organization. Llewellyn does not anticipate the features claimed in claim 16 of the present arrangement.

Llewellyn describes enabling remote access and control of applications located at multiple locations. Multiple users can access and control the same instance of a running application. A provider of a particular service may see a user's screen and control the computer of a user. Llewellyn does not disclose or suggest a "particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization following login to said application and without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 16 of the present arrangement. Llewellyn, contrary to the present arrangement,

employs an administrator of a server farm (*see* fig. 2, reference no. 99) such as an **application service provider administrator** to manage user accounts. Llewellyn describes

> "an application program that would execute entirely on a server computer and enable one remote user to see and control the screen of a second remote user. Such a system would preferably include ... the ability for multiple users of an application to use a single instance of the application ... providing a distinct functionality or functionalities to the second and subsequent remote users" (paragraph [0027]).

Thus Llewellyn merely allows an application service provider to access an application program. Therefore, Llewellyn neither discloses nor suggests a "particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization following login to said application and **without intervention by the application service provider**" or "**excluding access** to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 16 of the present arrangement.

In the present claimed arrangement, "system 100 enables individual organizations 104 of multiple different organizations to manage access of employees to a remotely located application 123 hosted by an application service provider" (specification, page 9, lines 27-29). Thereby:

> "The customer account management (CAM) system 100 **advantageously** provides efficient and secure intranet and Internet access for customer administrators at organizations 104, such as hospitals, to **manage their own application user accounts**. The system 100 restrict access so that customer account administrators have no access to user accounts assigned to other organizations, preferably by adding a prefix representing the parent organization in order to establish uniqueness. The system 100 permits customers to **self-sufficient to manage their own application user accounts, without requiring intervention** by or cooperation with another party. The system 100 provides real time savings for customers, and requires less staff time at the ASP support help desk to perform account management functions" (specification, page 31, lines 7-16).

Thus, the present claimed arrangement recites a "particular executable procedure" that supports a "user in managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization following login to said application and **without intervention by the application service provider** and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization." This is neither suggested nor disclosed by the system of Llewellyn.

Moreover, Llewellyn in cited paragraph [0109] describes that

> "[t]he server configuration module 196 may enable an **administrator** of a server station 100 to specify security measures for a server. Security measures may include permissions for accessing files or functionality of a server module 160. The server configuration module 196 may also enable an administrator to **set up accounts** which may include authentication and configuration data associated with a particular user or **organization**" (paragraph [0109]).

Thus, the "administrator of a server station 100" is an Application Service Provider administrator and the administrator controls the operations performed by the system of Llewellyn. Therefore, Llewellyn **teaches directly away** from the claimed "user of a particular organization of said plurality of organizations in managing access ... **without intervention by the application service provider.**" Moreover, Llewellyn in paragraph [0077] describes "[a] server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide **centralized administration** and horizontal scaleability." This is wholly unlike and is in direct contrast to the distributed access management by users of individual particular organizations "of said plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by said plurality of organizations" as recited in claim 16 of the present arrangement.

Furthermore, Llewellyn teaches the advantages of centralized management of user access and fails to recognize the problem addressed by the claimed arrangement. Specifically, Llewellyn states:

> [t]he server farm 99 may be an Application Service Provider ('ASP') farm 99. **An ASP typically deploys, hosts, and manages access to an application**, such as an application 86, to multiple users from a centrally managed facility. An ASP also typically delivers applications 86 over networks 30, 50 on a subscription basis. Moreover, **ASPs are designed to speed implementation of new applications, minimize the expenses and risks borne over an application's life cycle**, and ameliorate the problems associated with the current shortage of qualified technical personnel in the marketplace" (paragraph [0078]).

Thus, in Llewellyn, an ASP manages access to an application. Moreover, Llewellyn describes the "[b]enefits of **application server computing** include **single-point management**, universal application access, bandwidth-independent performance, and **improved security** for business applications" (paragraph [0077]). Therefore, Llewellyn is concerned with "a system administrator [that] may be a provider [i.e. Application Service Provider] ... while the

users of the system may be subscribers," (paragraph [0193]). Llewellyn neither discloses nor suggests "the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization following login to said application and **without intervention by the application service provider** and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 16 of the present arrangement.

Furthermore, cited paragraph [0092] of Llewellyn describes that "[t]he entry point management module 148 may also maintain connections between users and entry points, allowing users to access data and functionality specific to their session with an application 86." Cited paragraph [0176] describes that "[e]ach user interface 482a,b may be different and allow access to data 484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a." However, as described above, the system of Llewellyn is managed by an Application Service Provider. Therefore, Llewellyn neither discloses nor suggests "the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization following login to said application and without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 16 of the present arrangement. Consequently, it is respectfully requested that the rejection of claim 16 under 35 U.S.C. 102(e) be withdrawn.

CLAIMS 17 and 18

Independent claim 17 provides a system enabling individual organizations of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider. At an application service provider site, at least one database contains data representing an image associated with a corresponding plurality of organizations and a plurality of executable procedures associated with the corresponding plurality of user interface images. An executable procedure supports a user of a particular organization of the plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by the plurality of organizations. At least one repository includes data representing an application and associated application data specific to the particular organization. An authorization processor authorizes

access of the user to a particular user interface image and an associated particular executable procedure associated with the particular organization in response to received identification information of the user and excludes access of the user and employees of the particular organization to user interface images and executable procedures and data associated with the organizations other than the particular organization. A command processor employs the at least one database for initiating execution of a particular executable procedure in response to a command initiated at a remote location associated with the particular organization using a particular user interface image associated with the particular executable procedure and with the particular organization. The particular executable procedure supports the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to the particular organization without intervention by the application service provider and excludes access to the application data specific to the particular organization by employees of organizations other than the particular organization. Llewellyn does not anticipate the features claimed in claim 17 of the present arrangement.

Llewellyn describes enabling remote access and control of applications located at multiple locations. Multiple users can access and control the same instance of a running application. A provider of a particular service may see a user's screen and control the computer of a user. Llewellyn does not disclose or suggest a "particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 17 of the present arrangement. Llewellyn, contrary to the present arrangement, employs an administrator of a server farm (*see* fig. 2, reference no. 99) such as an **application service provider administrator** to manage user accounts. Llewellyn describes

> "an application program that would execute entirely on a server computer and enable one remote user to see and control the screen of a second remote user. Such a system would preferably include ... the ability for multiple users of an application to use a single instance of the application ... providing a distinct functionality or functionalities to the second and subsequent remote users" (paragraph [0027]).

Thus Llewellyn merely allows an application service provider to access an application program. Therefore, Llewellyn neither discloses nor suggests a "particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization **without intervention by the application service provider**" or

"**excluding access** to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 17 of the present arrangement.

In the present claimed arrangement, "system 100 enables individual organizations 104 of multiple different organizations to manage access of employees to a remotely located application 123 hosted by an application service provider" (specification, page 9, lines 27-29). Thereby:

> "The customer account management (CAM) system 100 **advantageously** provides efficient and secure intranet and Internet access for customer administrators at organizations 104, such as hospitals, to **manage their own application user accounts**. The system 100 restrict access so that customer account administrators have no access to user accounts assigned to other organizations, preferably by adding a prefix representing the parent organization in order to establish uniqueness. The system 100 permits customers to **self-sufficient to manage their own application user accounts, without requiring intervention** by or cooperation with another party. The system 100 provides real time savings for customers, and requires less staff time at the ASP support help desk to perform account management functions" (specification, page 31, lines 7-16).

Thus, the present claimed arrangement recites a "particular executable procedure" that supports a "user in managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization following login to said application and **without intervention by the application service provider** and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization." This is neither suggested nor disclosed by the system of Llewellyn.

Moreover, Llewellyn in cited paragraph [0109] describes that

> "[t]he server configuration module 196 may enable an **administrator** of a server station 100 to specify security measures for a server. Security measures may include permissions for accessing files or functionality of a server module 160. The server configuration module 196 may also enable an administrator to **set up accounts** which may include authentication and configuration data associated with a particular user or **organization**" (paragraph [0109]).

Thus, the "administrator of a server station 100" is an Application Service Provider administrator and the administrator controls the operations performed by the system of Llewellyn. Therefore, Llewellyn **teaches directly away** from the claimed "user of a particular organization of said plurality of organizations in managing access ... **without**

intervention by the application service provider." Moreover, Llewellyn in paragraph [0077] describes "[a] server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide **centralized administration** and horizontal scaleability." This is wholly unlike and is in direct contrast to the distributed access management by users of individual particular organizations "of said plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by said plurality of organizations" as recited in claim 17 of the present arrangement.

Furthermore, Llewellyn teaches the advantages of centralized management of user access and fails to recognize the problem addressed by the claimed arrangement. Specifically, Llewellyn states:

> [t]he server farm 99 may be an Application Service Provider ('ASP') farm 99. **An ASP typically deploys, hosts, and manages access to an application**, such as an application 86, to multiple users from a centrally managed facility. An ASP also typically delivers applications 86 over networks 30, 50 on a subscription basis. Moreover, **ASPs are designed to speed implementation of new applications, minimize the expenses and risks borne over an application's life cycle**, and ameliorate the problems associated with the current shortage of qualified technical personnel in the marketplace" (paragraph [0078]).

Thus, in Llewellyn, an ASP manages access to an application. Moreover, Llewellyn describes the "[b]enefits of **application server computing** include **single-point management**, universal application access, bandwidth-independent performance, and **improved security** for business applications" (paragraph [0077]). Therefore, Llewellyn is concerned with "a system administrator [that] may be a provider [i.e. Application Service Provider] ... while the users of the system may be subscribers," (paragraph [0193]). Llewellyn neither discloses nor suggests "the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization **without intervention by the application service provider** and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 17 of the present arrangement.

Furthermore, cited paragraph [0092] of Llewellyn describes that "[t]he entry point management module 148 may also maintain connections between users and entry points, allowing users to access data and functionality specific to their session with an application 86." Cited paragraph [0176] describes that "[e]ach user interface 482a,b may be different and

allow access to data 484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a." However, as described above, the system of Llewellyn is managed by an Application Service Provider. Therefore, Llewellyn neither discloses nor suggests "the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 17 of the present arrangement. Consequently, it is respectfully requested that the rejection of claim 17 under 35 U.S.C. 102(e) be withdrawn.

In view of the above remarks, Applicants respectfully submit that Llewellyn does not anticipate the features claimed in the present claimed arrangement. Additionally, as claim 18 is dependent on independent claim 17, claim 18 is considered patentable for the reasons presented above with respect to claim 17. Consequently, it is respectfully submitted that the rejection of claim 18 under 35 U.S.C. 102(b) be withdrawn.

CLAIM 19

Independent claim 19 provides a user interface system enabling individual organizations of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider. At an application service provider site and accessed via a firewall, at least one database is included. The at least one database contains data representing a plurality of sets of user interface images associated with a corresponding plurality of organizations and a plurality of executable procedures associated with the corresponding plurality of sets of user interface images. An executable procedure supports a user of a particular organization of the plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by the plurality of organizations. A command processor employs the at least one database for initiating execution of a particular executable procedure in response to a command initiated at a remote location associated with the particular organization using a user interface image selected from a set of images associated with a particular organization. The particular executable procedure supports the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to the particular organization without intervention by the application service provider and excludes access to the application data specific to the particular organization by employees of organizations

other than the particular organization. Llewellyn does not anticipate the features claimed in claim 19 of the present arrangement.

Llewellyn describes enabling remote access and control of applications located at multiple locations. Multiple users can access and control the same instance of a running application. A provider of a particular service may see a user's screen and control the computer of a user. Llewellyn does not disclose or suggest a "particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 19 of the present arrangement. Llewellyn, contrary to the present arrangement, employs an administrator of a server farm (*see* fig. 2, reference no. 99) such as an **application service provider administrator** to manage user accounts. Llewellyn describes

> "an application program that would execute entirely on a server computer and enable one remote user to see and control the screen of a second remote user. Such a system would preferably include ... the ability for multiple users of an application to use a single instance of the application ... providing a distinct functionality or functionalities to the second and subsequent remote users" (paragraph [0027]).

Thus Llewellyn merely allows an application service provider to access an application program. Therefore, Llewellyn neither discloses nor suggests a "particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization **intervention by the application service provider**" or "**excluding access** to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 19 of the present arrangement.

In the present claimed arrangement, "system 100 enables individual organizations 104 of multiple different organizations to manage access of employees to a remotely located application 123 hosted by an application service provider" (specification, page 9, lines 27-29). Thereby:

> "The customer account management (CAM) system 100 **advantageously** provides efficient and secure intranet and Internet access for customer administrators at organizations 104, such as hospitals, to **manage their own application user accounts**. The system 100 restrict access so that customer account administrators

> have no access to user accounts assigned to other organizations, preferably by adding a prefix representing the parent organization in order to establish uniqueness. The system 100 permits customers to **self-sufficient to manage their own application user accounts, without requiring intervention** by or cooperation with another party. The system 100 provides real time savings for customers, and requires less staff time at the ASP support help desk to perform account management functions" (specification, page 31, lines 7-16).

Thus, the present claimed arrangement recites a "particular executable procedure" that supports a "user in managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization following login to said application and **without intervention by the application service provider** and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization." This is neither suggested nor disclosed by the system of Llewellyn.

> Moreover, Llewellyn in cited paragraph [0109] describes that
>
> "[t]he server configuration module 196 may enable an **administrator** of a server station 100 to specify security measures for a server. Security measures may include permissions for accessing files or functionality of a server module 160. The server configuration module 196 may also enable an administrator to **set up accounts** which may include authentication and configuration data associated with a particular user or **organization**" (paragraph [0109]).

Thus, the "administrator of a server station 100" is an Application Service Provider administrator and the administrator controls the operations performed by the system of Llewellyn. Therefore, Llewellyn **teaches directly away** from the claimed "user of a particular organization of said plurality of organizations in managing access ... **without intervention by the application service provider**." Moreover, Llewellyn in paragraph [0077] describes "[a] server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide **centralized administration** and horizontal scaleability." This is wholly unlike and is in direct contrast to the distributed access management by users of individual particular organizations "of said plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by said plurality of organizations" as recited in claim 19 of the present arrangement.

Furthermore, Llewellyn teaches the advantages of centralized management of user access and fails to recognize the problem addressed by the claimed arrangement. Specifically, Llewellyn states:

> [t]he server farm 99 may be an Application Service Provider ('ASP') farm 99. **An ASP typically deploys, hosts, and manages access to an application**, such as an application 86, to multiple users from a centrally managed facility. An ASP also typically delivers applications 86 over networks 30, 50 on a subscription basis. Moreover, **ASPs are designed to speed implementation of new applications, minimize the expenses and risks borne over an application's life cycle**, and ameliorate the problems associated with the current shortage of qualified technical personnel in the marketplace" (paragraph [0078]).

Thus, in Llewellyn, an ASP manages access to an application. Moreover, Llewellyn describes the "[b]enefits of **application server computing** include **single-point management**, universal application access, bandwidth-independent performance, and **improved security** for business applications" (paragraph [0077]). Therefore, Llewellyn is concerned with "a system administrator [that] may be a provider [i.e. Application Service Provider] ... while the users of the system may be subscribers," (paragraph [0193]). Llewellyn neither discloses nor suggests "the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization **without intervention by the application service provider** and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 19 of the present arrangement.

Furthermore, cited paragraph [0092] of Llewellyn describes that "[t]he entry point management module 148 may also maintain connections between users and entry points, allowing users to access data and functionality specific to their session with an application 86." Cited paragraph [0176] describes that "[e]ach user interface 482a,b may be different and allow access to data 484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a." However, as described above, the system of Llewellyn is managed by an Application Service Provider. Therefore, Llewellyn neither discloses nor suggests "the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 19 of the present arrangement. Consequently, it is respectfully requested that the rejection of claim 19 under 35 U.S.C. 102(e) be withdrawn.

Rejection of claims 4-6, 8 and 9 under 35 U.S.C. 103(a)

Reversal of the rejection of claims 4-6, 8 and 9 under 35 U.S.C. 103(a) as being unpatentable over Llewellyn (U.S. Patent Pub. No. 2003/0061279 A1) in view of Gavrila (U.S. Patent Pub. No. 2002/0026592 A1) is respectfully requested because the rejection makes crucial errors in interpreting the cited reference. The rejection erroneously states that claims 4-6, 8 and 9 are unpatentable over Llewellyn in view of Gavrila.

CLAIMS 4 and 5

Claim 4 is dependent upon independent claim 1 and is allowable for the reasons presented above with respect to claim 1. Specifically, Llewellyn does not disclose or suggest the claimed features of the present arrangement. Additionally, Gavrila, when taken in combination with Llewellyn, also does not make the present claimed arrangement unpatentable.

Gavrila describes a method for automatic permission management in centralized and distributed operating systems using role-based access control that supports selective and multiple instantiations of roles, multiple inheritance of permission and membership, and provides scalable and efficient distribution, review, and revocation of permissions and access authorization. Gavrila (with Llewellyn) neither discloses nor suggests a "particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization following login to said application and without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 1 of the present arrangement. Gavrila is merely concerned with managing permissions in large centralized and distributed operating systems. Gavrila revokes "permissions for objects to roles rather than directly to individual users, and" controls "users' permissions by granting or revoking them membership to appropriate roles. Furthermore, users can be reassigned from one role to another, without requiring any explicit permission distribution or revocation action by administrators at the object level ... Roles can be granted new permissions as new applications and objects become accessible, and permissions can be revoked from roles whenever necessary" (paragraph [0005]). However, Gavrila is not concerned with and does not disclose or suggest "[a] system enabling individual organizations of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider ... the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application

and associated application data specific to said particular organization without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 1 of the present arrangement. Merely granting or revoking user membership to appropriate roles and reassigning roles without explicit permission by administrators, as in Gavrila (with Llewellyn) does not disclose or suggest the features of the present claimed arrangement. Therefore, Gavrila (with Llewellyn) does not make the present claimed arrangement unpatentable.

Llewellyn describes a **centralized** system in which an **administrator** specifies security measures for the sever. In direct contrast, Gavrila teaches away from the centralized system of Llewellyn. Gavrila teaches a Role-Based Access Control (RBAC) system, incompatible with the Llewellyn system, which facilities the management of permissions or large systems. Rather than authorizing a system administrator to set permissions, control the server, etc., Gavrila grants or revokes permissions for objects to **roles** rather than directly to individual users (*see* paragraphs [0004] and [0005] of Gavrila). Thus, the system of Llewellyn, which is controlled by a system administrator, is wholly unlike the roles-based system of Gavrila. Moreover, combining the two systems would yield an inoperable device. The combined system would not function because an administrator would attempt to set security permissions, etc. for the server (as in Llewellyn), however, the system would not take commands from individual users but would rather operate via Role-Based Access Control (as in Gavrila). Therefore, the combined system would be inoperable, as Llewellyn describes that an **administrator** is in control of permissions for a server, and Gavrila describes that a **role-based** system (controlled without the intervention of an administrator) grants or revokes access.

Even if the systems of Llewellyn and Gavrila were combined, as suggested by the Office Action, the combination would not make the present claimed arrangement unpatentable. The combined system would merely provide a centralized system for setting permissions on a server. An application service provider would be able to view and control different users computers. The combined system would allow multiple users to enter a single instance of the application program at different entry points. The combined system would also grant or revoke user membership to appropriate **roles** and reassign roles without the explicit permission of an **administrator**. However, the combined system, similar to the individual systems of Llewellyn and Gavrila would not disclose or suggest "particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization **without intervention by the application service provider**" or

"excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 1 of the present arrangement. Even if the combination of Llewellyn and Gavrila was operative, granting access to a role in a RBAC (Role-Based Access Control) system is not equivalent to and does not disclose or suggest "granting access of an employee of the particular organization to an application and associated application data specific to said particular organization" The combined system would be a system controlled by the application service provider and would also grant access according to roles. However, the combined system would not disclose or suggest "supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization **without intervention by the application service provider**" as recited in claim 1 of the present arrangement. Therefore, the combined system would not disclose or suggest " the particular executable procedure supporting the user in managing and granting access of an of an employee of the particular organization to an application and associated application data specific to said particular organization without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 1 of the present arrangement. As claims 4 and 5 are dependent upon these features, claims 4 and 5 are also allowable over Llewellyn and Gavrila. Consequently, it is respectfully requested that the rejection of claims 4 and 5 under 35 U.S.C. 103(a) be withdrawn.

CLAIM 6

Dependent claim 6 is dependent on claims 1 and 4 and is considered patentable for the reasons presented above with respect to claims 1 and 4. Additionally, claim 6 is also considered patentable because the features claimed are not made unpatentable by Llewellyn in view of Gavrila. Specifically, Llewellyn and Gavrila neither disclose nor suggest that "the authorization processor removes the permission of the user and employees of the particular organization in response to addition of the particular organization as a new organization to the plurality of organizations" as recited in claim 6 of the present arrangement.

The Office Action on page 24 argues that Gavrila, in paragraph [0032] describes adding a new permission-inheritance arc to the directed acyclic graph and automatically removing the role from the access control lists of all abstract objects accessible to that role. The Office Action further asserts that this operation in Gavrila (paragraph [0032]) is equivalent to automatically removing that role...when adding a new permission. Applicants respectfully disagree and fail to recognize the alleged equivalence. Merely adding a permission-inheritance arc, as in Gavrila, is unrelated to and does not disclose or suggest removing "the

permission of the user and employees of the particular organization in response to **addition of the particular organization as a new organization** to the plurality of organizations" as recited in claim 6 of the present arrangement. Gavrila is merely concerned with adding a new permission-inheritance arc between a first and a second role. Additionally, adding a new permission, as in Gavrila, is not equivalent to "**a new organization** to the plurality of organizations" as recited in claim 6 of the present arrangement. Therefore, Gavrila with Llewellyn does not make the present claimed arrangement as claimed in claim 6 unpatentable. Consequently, it is respectfully requested that the rejection of claim 6 under 35 U.S.C. 103(a) be withdrawn.

CLAIMS 8 and 9

Dependent claim 8 is dependent on claim 1 and is considered patentable for the reasons presented above with respect to claims 1 and 4. Additionally, claim 8 is also considered patentable because the features claimed are not made unpatentable by Llewellyn in view of Gavrila. Specifically, Llewellyn and Gavrila neither disclose nor suggest "an executable procedure enables the user to at least one of, (a) add an employee and (b) remove an employee, of an organization as a user entitled to access the application hosted by the application service provider" as recited in claim 8 of the present arrangement.

The Office Action on page 24 argues that "adding the member of the first role instance to the instance of a second role and to all instances of the roles that inherit the membership of the second role" described in paragraph [0197] is equivalent to the claimed arrangement. Applicants respectfully disagree. Merely adding a member of a first role to an instance of a second role, as in Gavrila is not the same as "an executable procedure enables the user to at least one of, (a) **add an employee** and (b) **remove an employee, of an organization** as a user entitled to access the application hosted by the application service provider" as recited in claim 8 of the present arrangement. The addition of a member of a first role is not equivalent to and does not disclose or suggest "add[ing] an employee" or "remove[ing] an employee, of an organization as a user entitled to access the application hosted by the application service provider" as recited in claim 8 of the present arrangement. Therefore, claim 8 is patentable over Llewellyn in view of Gavrila. As claim 9 is dependent on claim 8, claim 9 is considered patentable for the same reasons as claim 8. Consequently, it is respectfully requested that the rejection of claims 8 and 9 under 35 U.S.C. 103(a) be withdrawn.

In view of the above remarks, Applicants respectfully submit that Llewellyn and Gavrila, when taken alone or in combination, do not make the present claimed arrangement

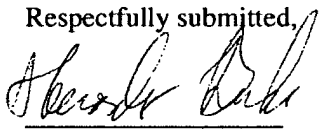
unpatentable. Consequently, it is respectfully submitted that the rejection of claims 4-6, 8 and 9 under 35 U.S.C. 103(a) be withdrawn.

VIII CONCLUSION

Llewellyn and Gavrila, when taken alone or in combination, neither disclose nor suggest "the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization" as recited in claim 1 of the present arrangement. Independent claims 16, 17 and 19 contain similar subject matter and are allowable for the same reasons as independent claim 1. Furthermore, as claims 2-15 and 18 are dependent on claims 1 17, respectively, these claims are also allowable over Llewellyn and Gavrila.

Accordingly it is respectfully submitted that the rejection of claims 1-19 should be reversed.

Respectfully submitted,



May 27, 2008

Alexander J. Burke
Reg. No. 40,425

Siemens Corporation
Customer No. 28524
Tel 732 321 3023
Fax 732 321 3030

APPENDIX I - APPEALED CLAIMS

1. (Previously Presented) A system enabling individual organizations of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider, comprising:

at an application service provider site,

at least one database containing data representing,

a plurality of user interface images associated with a corresponding plurality of organizations, and

a plurality of executable procedures associated with the corresponding plurality of user interface images, an executable procedure supporting a user of a particular organization of said plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by said plurality of organizations; and

a command processor employing the at least one database for initiating execution of a particular executable procedure in response to a command initiated at a remote location associated with the particular organization using a particular user interface image associated with the particular executable procedure and with the particular organization, the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization.

2. (Previously Presented) A system according to claim 1, wherein

said at least one database, said command processor, said application and associated application data specific to said particular organization are located at said application service provider site behind a firewall and accessed through said firewall by users of said plurality of organizations and including

an authorization processor for authorizing access of the user to the particular user interface image and the associated particular executable procedure in response to received identification information of the user.

3. (Previously Presented) A system according to claim 2, wherein

said particular executable procedure and said particular user interface image are specifically associated with said particular organization and

the authorization processor excludes access of the user and employees of the particular organization to user interface images and executable procedures and data associated with organizations other than the particular organization.

4. (Original) A system according to claim 3, wherein

the authorization processor excludes access to the user and employees of the particular organization to data associated with organizations other than the particular organization by removing permission of the user and employees of the particular organization to access the data associated with the other organizations from a directory of permissions used to control data access.

5. (Original) A system according to claim 4, wherein

the directory of permissions comprises a Microsoft compatible Active Control List (ACL).

6. (Original) A system according to claim 4, wherein

the authorization processor removes the permission of the user and employees of the particular organization in response to addition of the particular organization as a new organization to the plurality of organizations.

7. (Original) A system according to claim 1, wherein

the plurality of executable procedures comprises a plurality of sets of executable procedures associated with the corresponding plurality of user interface images and

the command processor employs the at least one database for initiating execution of a particular executable procedure in a particular set of executable procedures in response to a command initiated using the particular user interface image.

8. (Original) A system according to claim 1, wherein

an executable procedure enables the user to at least one of, (a) add an employee and (b) remove an employee, of an organization as a user entitled to access the application hosted by the application service provider.

9. (Original) A system according to claim 8, wherein

the executable procedure changes authorization information associated with the added or removed employee.

10. (Original) A system according to claim 1, wherein

an executable procedure enables the user to amend information used in authorizing a particular employee of an organization to access the application hosted by the application service provider.

11. (Original) A system according to claim 1, including

an authorization processor for authorizing access of the employee of the particular organization to the particular user interface image and the associated particular executable procedure in response to received employee identification information.

12. (Original) A system according to claim 11, wherein

the authorization processor uses a combination of an organization specific identifier and received employee identification information in providing an employee access to the application hosted by the application service provider to prevent replication of user identification information between two employees of different organizations of the plurality of organizations.

13. (Original) A system according to claim 1, wherein

an executable procedure comprises processor executable instruction in a computer language including at least one of, (a) assembly language, (b) machine code, (c) a compiled computer language, (d) an interpreted computer language, (e) a compilable computer language, (f) a script language and (g) hardware encoded logic.

14. (Original) A system according to claim 1, wherein

the particular executable procedure comprises a template procedure customized by at least one of, (a) the user and (b) a technician.

15. (Original) A system according to claim 1, wherein

at least one of, (a) the command is initiated at a user site via a particular user interface image communicated to the user site and (b) the particular executable procedure is communicated to a user site and executed at the user site.

16. (Previously Presented) A system enabling an individual organization of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider, comprising:

at an application service provider site,

a communication processor for accessing at least one database containing data representing,

a plurality of user interface images associated with a corresponding plurality of organizations, and

a plurality of executable procedures associated with the corresponding plurality of user interface images, an executable procedure supporting a user of a particular organization of said plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by said plurality of organizations;

at least one repository including data representing an application and associated application data specific to said particular organization; and

a command processor for using the communication processor in initiating execution of a particular organization specific executable procedure in response to a command initiated at a remote user site associated with the particular organization using a particular organization specific user interface image communicated to the user site, the particular user interface image being associated with the particular executable procedure and with the particular organization, the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization following login to said application and without intervention by the application service provider and excluding access

to said application data specific to said particular organization by employees of organizations other than said particular organization.

17. (Previously Presented) A system enabling individual organizations of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider, comprising:

at an application service provider site,

at least one database containing data representing,

a images associated with a corresponding plurality of organizations, and

a plurality of executable procedures associated with the corresponding plurality of user interface images, an executable procedure supporting a user of a particular organization of said plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by said plurality of organizations;

at least one repository including data representing an application and associated application data specific to said particular organization;

an authorization processor for authorizing access of the user to a particular user interface image and an associated particular executable procedure associated with the particular organization in response to received identification information of the user and excluding access of the user and employees of the particular organization to user interface images and executable procedures and data associated with the organizations other than the particular organization; and

a command processor employing the at least one database for initiating execution of a particular executable procedure in response to a command initiated at a remote location associated with the particular organization using a particular user interface image associated

with the particular executable procedure and with the particular organization, the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization.

18. (Original) A system according to claim 17, wherein

the authorization processor authorizes access of the user in response to a command initiated using the particular user interface image.

19. (Previously Presented) A user interface system enabling individual organizations of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application service provider, comprising:

at an application service provider site and accessed via a firewall,

at least one database containing data representing,

a plurality of sets of user interface images associated with a corresponding plurality of organizations, and

a plurality of executable procedures associated with the corresponding plurality of sets of user interface images, an executable procedure supporting a user of a particular organization of said plurality of organizations in managing access of employees of the particular organization to an application hosted by an application service provider and used by said plurality of organizations; and

a command processor employing the at least one database for initiating execution of a particular executable procedure in response to a command initiated at a remote location associated with the particular organization using a user interface image selected from a set of images associated with a particular organization, the particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to an application and associated application data specific to said particular organization without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization.

APPENDIX II - EVIDENCE

Applicant does not rely on any additional evidence other than the arguments submitted hereinabove.

APPENDIX III - RELATED PROCEEDINGS

Applicant respectfully submits that there are no proceedings related to this appeal in which any decisions were rendered.

APPENDIX IV - TABLE OF CASES

APPENDIX V - LIST OF REFERENCES

U.S. Pub. No.	Issued Date	102(e) Date	Inventors
2003/0061279 A1			Llewellyn et al.
2002/0026592 A1			Gavrila et al.

TABLE OF CONTENTS

ITEMS		PAGE
I.	Real Party in Interest	2
II.	Related Appeals and Interferences	2
III.	Status of Claims	2
IV.	Status of Amendments	2
V.	Summary of the Claimed Subject Matter	2-6
VI.	Grounds of Rejection to be Reviewed on Appeal	6
VII.	Argument	6-27
VIII	Conclusion	28

APPENDICES

I.	Appealed Claims	29-37
II.	Evidence	38
III.	Related Proceedings	39
IV.	Table of Cases	40
V.	List of References	40